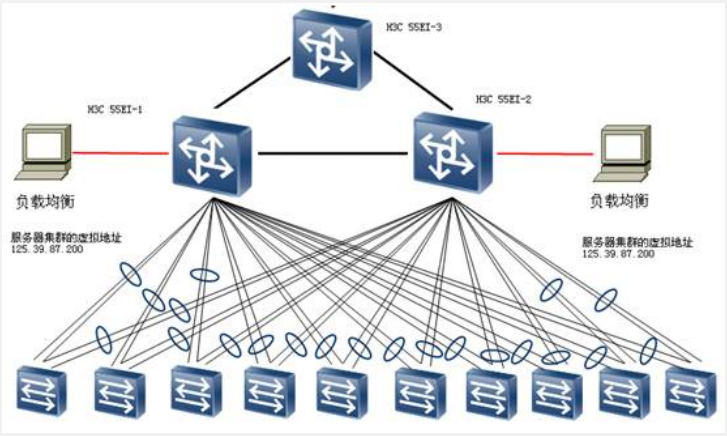
S5500/S5800系列交换机在VLAN或VLAN虚接口下发访问控制导致报文转发不通的问题

王晨【技术大咖】 2009-08-17 发表

S5500/S5800系列交换机在VLAN和VLAN虚接口下发访问控制导致报文转发不通的问题

一、 组网：



用户对外公布一个DNS映射： 125.39.87.200-网页。外网发起访问服务时，目的地址为125.39.87.200，报文经S55EI-3，先在汇聚层S5500-EI上进行三层转发，然后到达负载均衡器，由均衡器选择接入层下服务器机群中的一台服务器，将报文的目的地址替换为此服务器的IP地址，然后再进行二层转发，报文由服务器始发回程的时候，报文源封装具体服务器的地址，不经过负载均衡器，直接经汇聚层S5500-EI三层转发到S55EI-3。

二、 问题描述：

用户需求是保证只有访问125.39.87.200的www服务的报文才能进入交换机，但在具体下发过程中，用户发现，在S5500交换机上的vlan内下发访问控制后，外网PC不能正常访问服务器的www服务，但在其他局点的S5800交换机上在Vlan接口上下发访问控制，就可达到用户的目的。

三、 过程分析：

55EI上配置如下:

```
acl number 3000
 rule 0 permit ip source 125.39.87.0 0.0.0.255
rule 1 permit tcp destination 125.39.87.200 0 destination-port eq www
acl number 3001
 rule 0 deny ip
traffic behavior B
 filter permit
traffic behavior D
 filter deny
qos policy ABCD
 classifier A behavior B
 classifier C behavior D
qos apply policy ABCD vlan 2 outbound
```

S5800上配置的策略与S5500-EI上一致，只是S5800在vlan 接口上下发QoS策略。

```
acl number 3000
 rule 0 permit ip source 1.1.1.0 0.0.0.255
rule 205 permit tcp destination 119.97.134.230 0 destination-port eq www rule 215 d
eny ip
interface Vlan-interface2
  packet-filter 3000 outbound
```

S5500-EI上下发的访问控制，是在vlan下下发，也就是说访问控制将对经过vlan 2的三层流和二层流都起作用，而在S5800交换机上vlan接口上下发的访问控制，将只对vlan 2的三层流起作用，二层流将不进行检测。现在我们来看一下S5500-EI上是如何出现问题的：外网一个访问服务器网页的数据流，根据DNS解析后，生成一条目的地址为125.39.87.200的数据流，报文经S55EI-3后到S55EI-2(1)进行三层转发到均衡器，由均衡器将起目的地址替换为125.39.87.1（服务器机群中的一台服务器地址）后，进行二层转发，因楼层交换和汇聚层交换机S5500-EI之间配置了STP，阻塞了楼层交换和

S55EI-2的链路，报文需要经S55EI-1转发至下面的楼层交换，但此时目的地址为125.39.87.1的数据流到达S55EI-1后将因为没有被允许被丢弃，而同样的组网因S5800交换机的策略下发在vlan interface下，将不会检查二层流量，数据流将会被允许通过，因此造成了S5500-EI上有问题而S5800上没有问题的现象

四、 解决方法：

1， 将S5500-EI升级至2202P05版本后，将可以支持在vlan 虚接口上下发策略

2， 如不方便升级，可以上面的classifier A和C增加配置if-match source-mac “设备虚接口mac”与原有访问控制做与，也可以解决问题。